DEOSの最新動向とD-Case事例紹介

2013年10月22日

科学技術振興機構
DEOSC　屋代　眞

http://www.dependable-os.net/

独立行政法人
科学技術振興機構
Japan Science and Technology Agency

本日のお話しの内容

1. ディペンダビリティとD-Case
   - Open Systems Dependability
   - ディペンダビリティにおけるD-Caseの役割
   - D-Caseツール
2. D-Case事例
   - M銀行システム障害
   - PC遠隔操作による誤認逮捕
   - T証のシステム障害
3. D-CaseとSysML開発環境の連携
4. DEOSプロジェクト
   - DEOSプロジェクト成果物紹介
   - 標準化活動
   - ET2013
   - コンソーシアム　－　DEOS協会
5. まとめ

新たなディペンダビリティの考え方

オープンシステムディペンダビリティ（OSD）

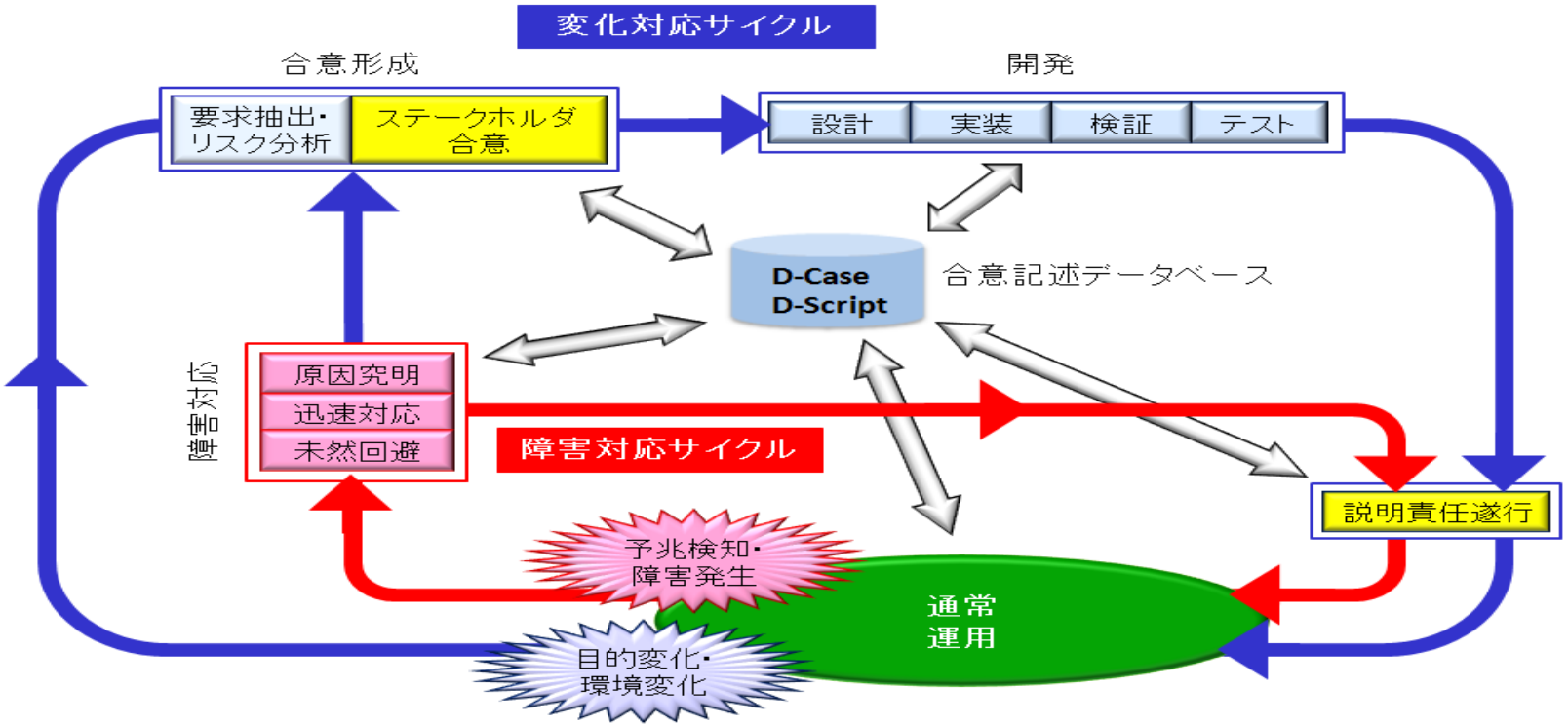
- **利用者がシステムに期待する便益を安全にかつ継続的に提供できる**
  - システム運用開始後の要求の変化に適応できる（**変化対応**）
  - システムの障害要因を顕在化する前にできる限り取り除くことができる（**未然防止**）
  - 障害が顕在化した後に迅速かつ適切に対応し、影響を最小とすることができる（**障害対応**）
- **ステークホルダーや社会への説明責任を全うできる**
  - 全ライフサイクルでの要求と実現に関する合意形成の構造的記録と履歴がある（**合意履歴保持**）
  - 合意に基づいたシステムの運用状況の監視と詳細な記録がある（**監視と記録**）

OSDを達成するためのコア技術

- **DEOSプロセス： ディペンダブルな開発運用のためのプロセス**
- **D-Case： 説明責任全うのための構造的表記法**

DEOSプロセス

- 反復的アプローチ
  - 目的や環境の変化に対してシステムを継続的に変更して行くための変化対応サイクル
  - 障害に対して迅速に対応するための障害対応サイクル
  - 障害対応サイクルから変化対応サイクルへのパス
- D-Caseを用いた合意記述データベースにより合意形成および開発・運用フェーズの統合と説明責任の全うを支援
- DEOSプロセスの考え方は2013年7月にThe Open Groupが標準として採用(*)

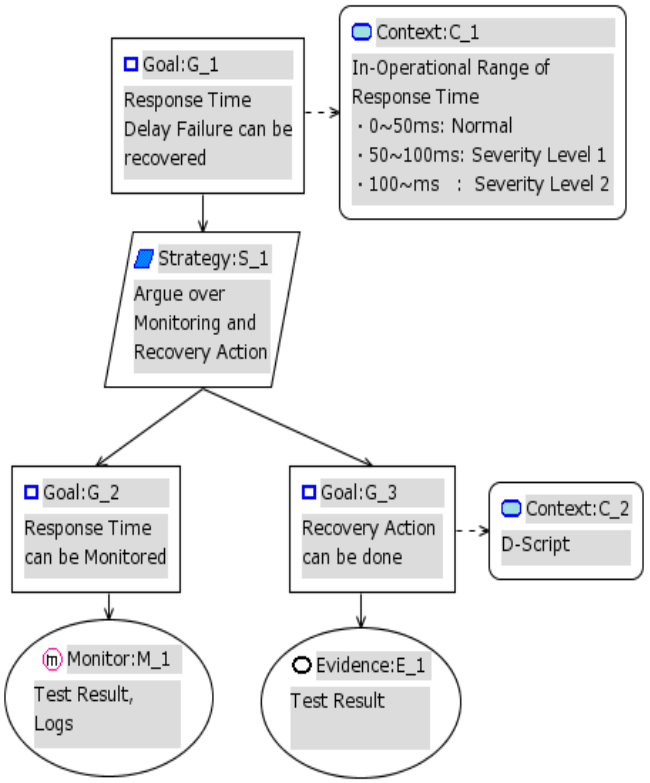


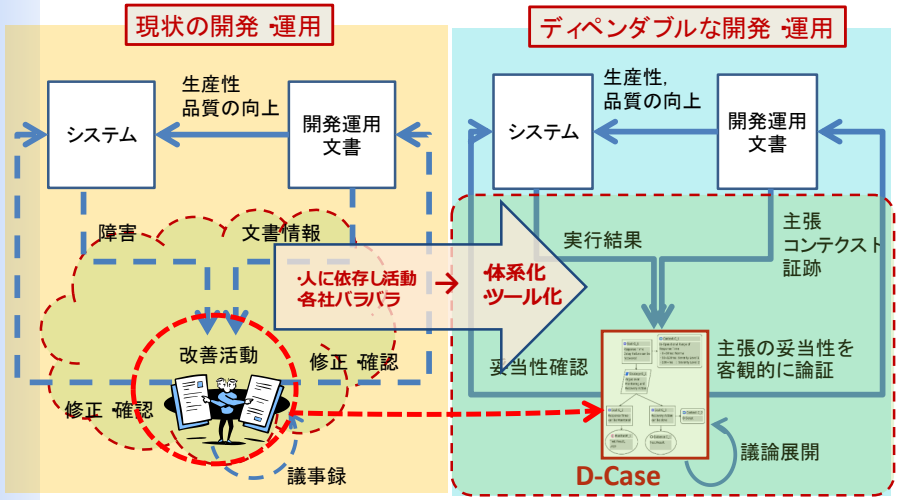
(*) Dependability through Assuredeness™ (O-DA) Framework (https://www2.opengroup.org/ogsys/catalog/c13f)

D-Case

- GSN (Goal Structuring Notation) をベースとした合意形成のための表記法
- GSNを拡張し、システムの運用状況の監視と詳細な記録を実現
- 開発・運用を含む全ライフサイクルでのステークホルダー間の合意形成
- D-Case記述の合意に基づく変更履歴が説明責任遂行を支援

D-Caseの記述例

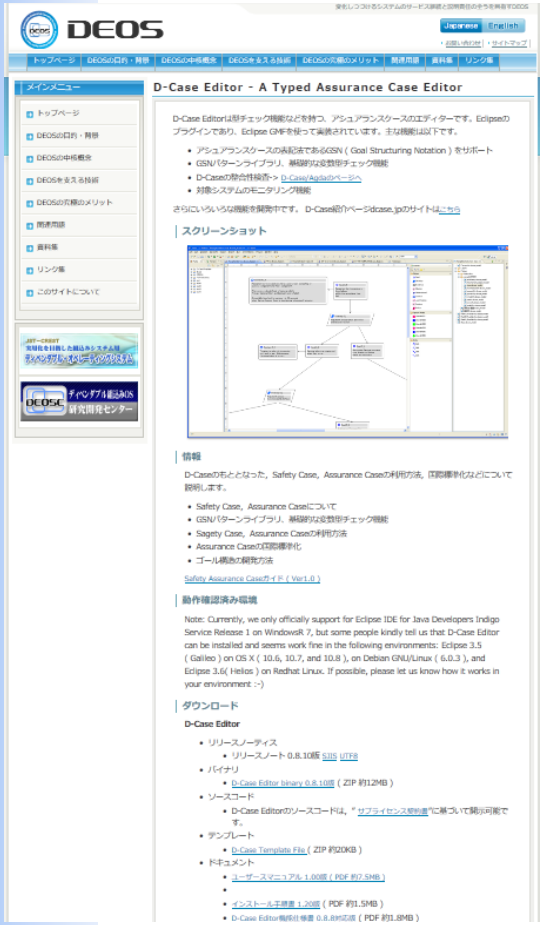


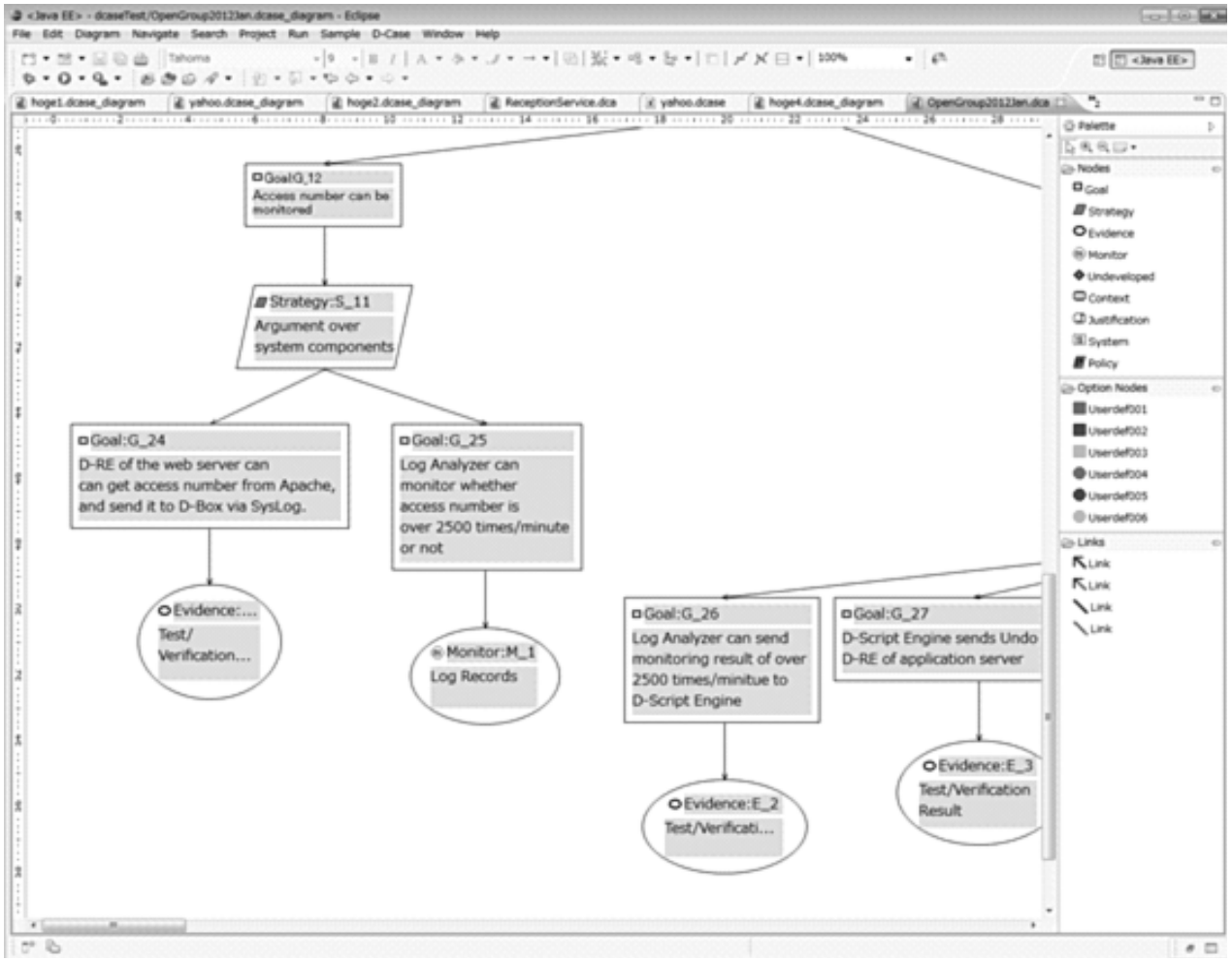


- D-Caseの活用により、属人性の強い改善活動から、体系化・ツール化されたプロセスへ

D-Case Editor

http://www.dependable-os.net/tech/D-CaseEditor/index.html





D-Case Weaver

http://www.dependable-os.net/tech/DCaseWeaver/index.html

変化しつづけるシステムのサービス継続と説明責任の全うを目指すDEOS

DEOS

Japanese English

お問い合わせ | サイトマップ

トップページ | DEOSの目的・背景 | DEOSの中核概念 | DEOSを支える技術 | DEOSの究極のメリット | 関連用語 | 資料集 | リンク集

メインメニュー

- トップページ
- DEOSの目的・背景
- DEOSの中核概念
- DEOSを支える技術
- DEOSの究極のメリット
- 関連用語
- 資料集
- リンク集
- このサイトについて

JST-CREST 実用化を目指した組込みシステム用 ディペンダブル・オペレーティングシステム

DEOSC ディペンダブル組込みOS 研究開発センター

D-Case Weaver

Web Browser上で

- D-CaseのGSNグラフを作成し、NodeやLinkを追加、変更、削除できます
- D-Caseの部分木をモジュール化することができます。またD-Caseへモジュールを追加することができます
- NodeにD-Scriptに関する情報を追加、変更、削除できます
- D-Case Weaverが生成するD-CaseのXML表現はD-Case Editorが生成するXML表現に対し、上位互換（スーパーセット）です
- GSNグラフのNodeのタイプ毎の統計情報を表示できます
- コンテンツマネージメントシステムAlfresco（Community版）と連携し、D-Case及びエビデンス文書の管理ができます
- Nodeに関連資料へのURLを添付（Attach）できます

Client / Server 環境（動作確認済み環境）

- Server

  OS：Ubuntu 12.04

  Http Server：Apache

- Client

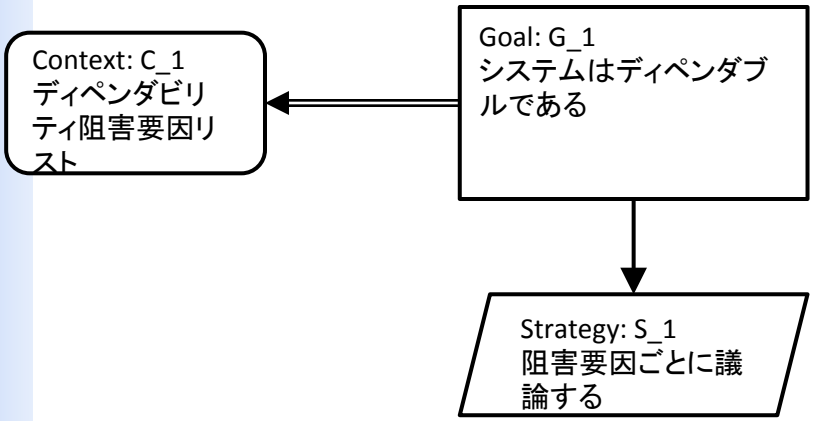
  OS：Ubuntu 12.04, Windows 7

  Browser：Firefox（Version 20.0）, Chrome（Version 26.0）

  ※Internet Explorerではご利用頂けません

D-Case Stencil for PowerPoint

http://www.dependable-os.net/tech/D-CaseStencil/index.html



D-Case事例　M銀行システム障害（2011年）の概要

- 2011年3月11日（金）に発生した東日本大震災発生に伴い、14日（月）におけるA社の義援金口座a、及び、15日（火）におけるB社の義援金口座bという特定の口座にそれぞれ大量の振込が集中したことにより、夜間バッチが異常終了したことに端を発し、以下の障害が発生した
- 障害内容（顧客へのサービスやビジネスに対し多大な影響を与えた）

1. **給与振込等の為替送信の遅延(のべ250万件、3/14～3/24)**
2. **営業店業務の取引開始遅延及び取引停止(3/15～3/25)**
   - 取引開始時刻の遅延（3/15（火）、16（水）、17（木））
   - 融資、ローン及び外国為替の取引停止（3/15（火）～3/22（火））
   - ローンの条件変更及び全額回収に係る取引停止（3/15（火）～3/25（金））
3. **ATMの利用停止及び利用制限（3/16（水）～3/23（水））**
4. **ダイレクトチャネルの利用制限**
   - みずほダイレクト（3/16（水）14:30～3/17（木）10:30、3/17（木）14:30～3/22（火）12:00 ）
   - e-ビジネスサイト及び法人向けEB（ 3/16（水）、3/17（木）8:00 ～11:30、3/17（木）19:00～3/22（火）12:00 ）
5. **営業店窓口での特定支払対応（3/19（土）～3/21（月・祝））**
6. **その他**
   - 取引明細の欠落
   - 口座振替における処理不能、誤った結果のデータ還元及び処理漏れ
   - その他夜間バッチの中段に伴う取引内容の不具合
   - 特例支払対応の未回収

システム障害の原因分析

1. 夜間バッチ異常終了と為替送信の遅延の原因（システム機能）
   - **大量取引が集中した場合のシステム処理単位**
     - 大量明細がある場合の後続の夜間バッチへのデータ振り分け処理量がリミット値を超越した
   - **夜間バッチが長期化した際のシステム運用機能**
     - 夜間バッチの長期化への対処である夜間バッチ中断することにより、その後の処理が膨大な手数を要することや為替送信が遅延する仕組みに対する対応策をあらかじめ検討していなかった
2. 復旧時の不手際の原因（復旧対応における緊急時態勢）
   - **緊急時における態勢が実効性を伴っていなかった**
   - **システムコンティンジェンシープランとして想定すべき事象が不足していた**
   - **復旧対応の手順書が実効性を伴っていなかった**
   - **チェックプロセス及び訓練が上記の実効性を検証する役割を果たせていなかった**
3. 通常運用時の点検不備の原因

（未然防止に向けたシステムリスク管理）

- **定期的システムリスク評価及び新商品・サービス導入時のシステムリスク評価の点検項目の見通しが不十分であった**

（経営管理及び監査）

- **人材の計画育成および適所配置の視点が希薄であった**
- **監査体制の不備や外部監査の活用の遺漏**

大量振込などの変化する要件への対応には、異常発生時にもサービスが継続するような仕組みが必要である

システム障害原因に対応するD-Case適用のポイント

＜適用にあたっての基本的な考え方＞

- 異常時のケースを全て明らかにするのではなく、異常発生時でも影響の最小化やサービス継続を進めるためのケースを明らかにする

障害原因

復旧時の不手際の原因（復旧対応における緊急時態勢）

- 緊急時における態勢が実効性を伴っていなかった
- システムコンティジェンシープランとして想定すべき事象が不足していた
- 復旧対応の手順書が実効性を伴っていなかった
- チェックプロセス及び訓練が上記の実効性を検証する役割を果たせていなかった

夜間バッチ異常終了と為替送信の遅延の原因（システム機能）

- 大量取引が集中した場合のシステム処理単位
  - 夜間バッチへのリミット値を超越した
- 夜間バッチが長期化した際のシステム運用機能
  - 夜間バッチ中断することにより、その後の処理が膨大な手数を要することや為替送信が遅延する仕組みに対する対応策をあらかじめ検討していなかった

通常運用時の点検不備の原因

（未然防止に向けたシステムリスク管理）

- 定期的システムリスク評価及び新商品・サービス導入時のシステムリスク評価の点検項目の見通しが不十分であった

（経営管理及び監査）

- 人材の計画育成および適所配置の視点が希薄であった
- 監査体制の不備や外部監査の活用の遺漏

D-Case適用ポイント

システム機能へのD-Caseの適用

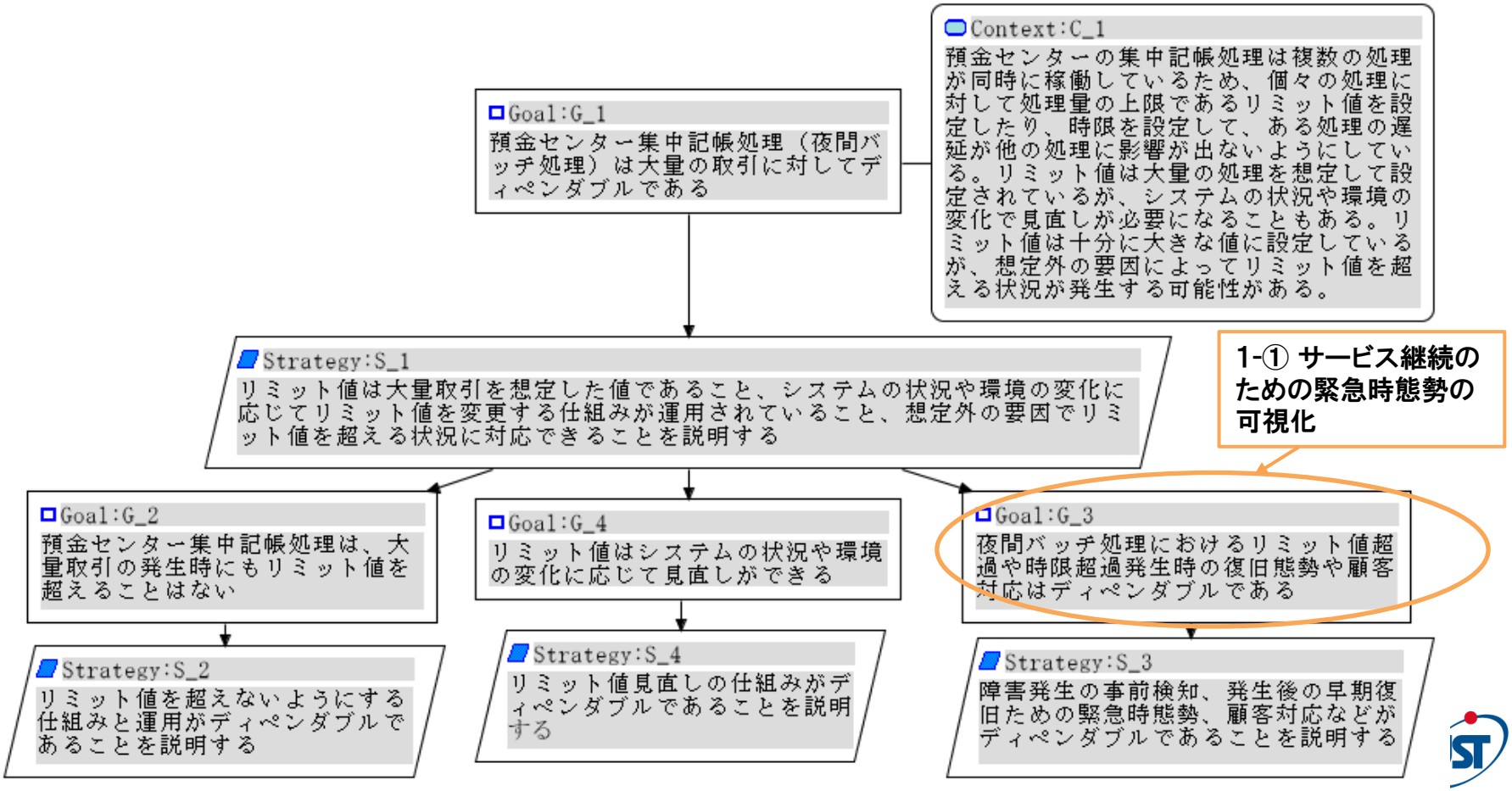
システム機能以外へのD-Caseの適用

1. サービス継続のための緊急時態勢の可視化
   - ① リミット値の超越や夜間バッチ処理の中断などの異常時でもサービスを継続するための運用を含むケースを明確化
   - ② ステークホルダーとの合意
   - ③ 実施担当者の明確化

2. 通常運転時のモニタリング
   - D-Caseのエビデンスやモニタを用いて、システムリスク評価の点検結果や人材のスキルや人材配置の点検結果、監査結果や外部監査結果などの可視化

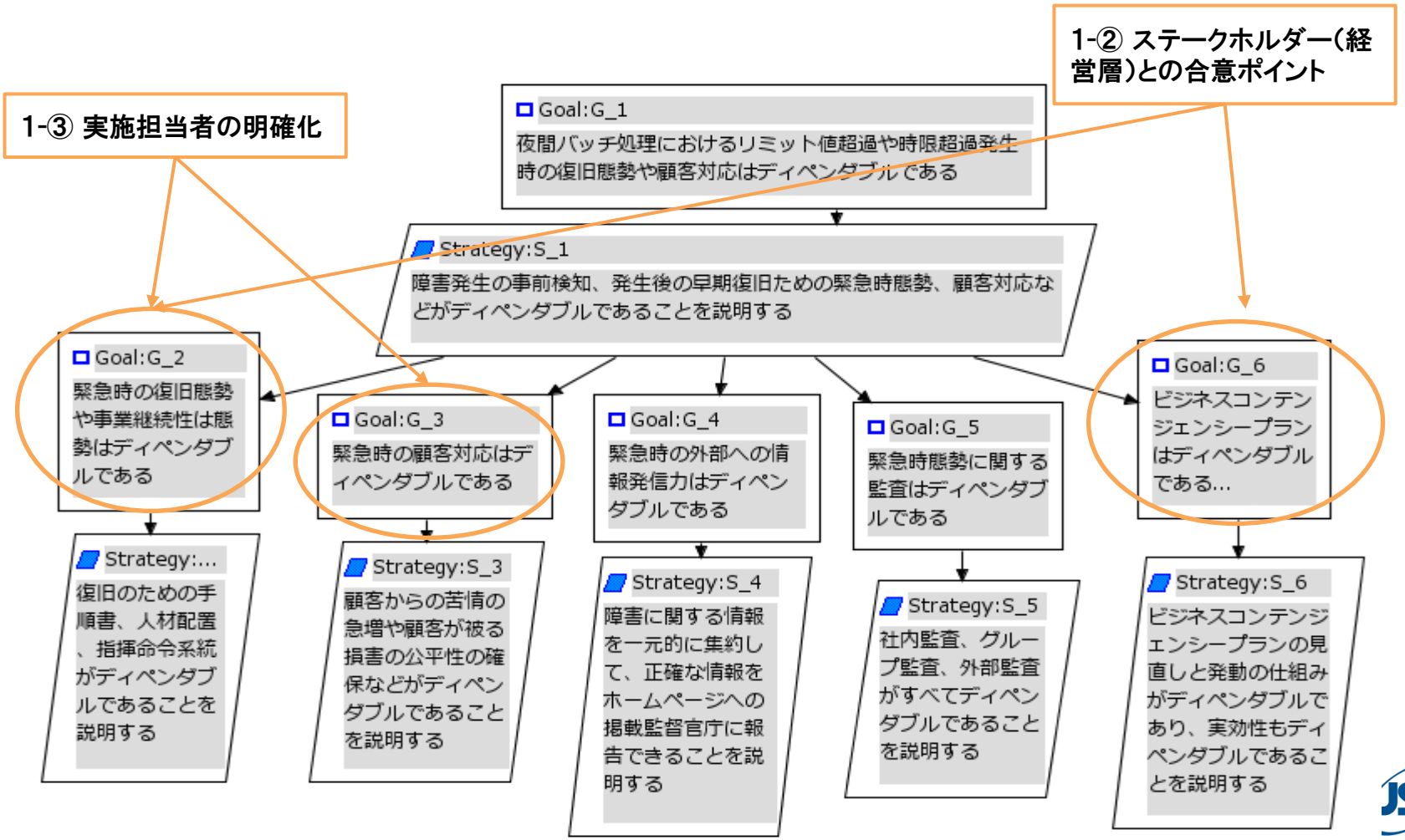
システム障害事例へのD-Case適用時の有効性（1/3）

- トップゴールの展開： 集中記帳処理(夜間バッチ処理)のケース(抜粋)
  - 経営上、システムにリミット値を持たせる選択の元、G_2:リミット値内での処理のケース、G_4:リミット値の見直しのケース、G_3:リミット値超過や時限超過が発生するケース、とすべての条件を網羅したゴール設定を行い、分析を実施



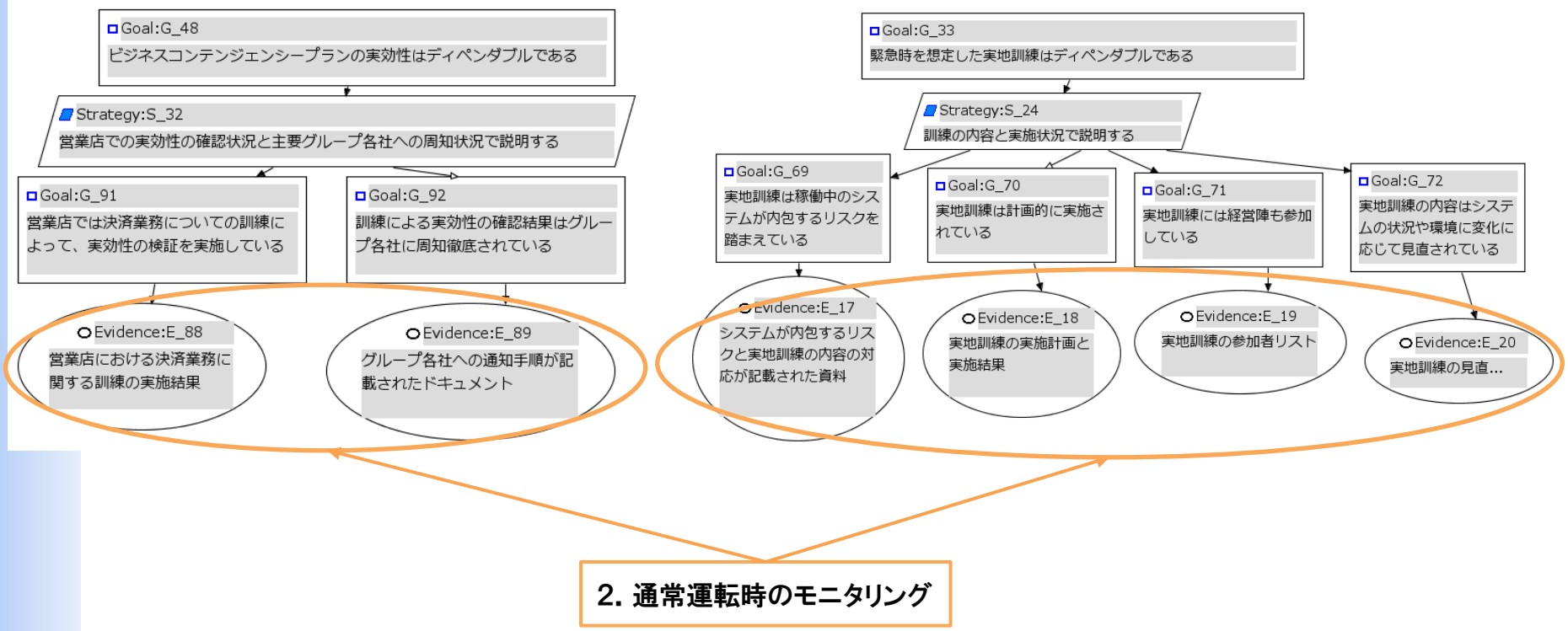
システム障害事例へのD-Case適用時の有効性（2/3）

- 人的展開が必要なリミット値越えの展開： 集中記帳処理(夜間バッチ処理)のケース(抜粋)
  - ゴールと戦略の合意を行うべきステークホルダや合意のポイント、それを行う実施担当者の明確化を実施



システム障害事例へのD-Case適用時の有効性（3/3）

- D-Case記述内容が信頼できるエビデンスで終端： 集中記帳処理(夜間バッチ処理)のケース(抜粋)
  - リミット値超過や時限超過が発生するケースでも、訓練実施結果や参加者リストなど、通常運転時に確認できるビジネスコンティンジェンシープランのエビデンスで終端し、実効性のモニタリング



システム障害事例へのD-Case適用のまとめ

D-Case適用
により

- 網羅性の可視化： システム機能の分析だけではカバーできない、人的対応部分も含め、サービス継続のための緊急時体制を可視化できる
  - （適用事例での例） リミット値超過や時限超過が発生するケースを分析
- 責任者の総覧化・可視化： D-Caseの1ドキュメント上に、ゴール毎に、経営層を含む実施担当者、合意したステークホルダーを明確化できる
  - （適用事例での例）
    - 実施担当者： 経営判断：経営者、復旧態勢や顧客対応：各実施責任者
    - 合意ポイント： 合意ステークホルダ、緊急時や事業継続性の態勢、ビジネスコンティンジェンシープラン
- 通常運転時確認可能なエビデンスで終端： D-Caseの最終ゴールのエビデンスは通常運転時にモニタリングできる内容として明確化することができる
  - （適用事例での例）ビジネスコンティンジェンシープランの実効性のモニタリング

その結果

- 異常（障害）発生時の迅速な対応と顧客サービスへの影響の最小化の実現
- 経営層を含むステークホルダーとの合意形成の容易化と可視化の実現
- 障害発生時の説明内容の可視化と説明責任の容易化の実現

D-Case事例　PC遠隔操作による誤認逮捕（2012年）の概要

1. 遠隔ウィルスによるトラブル発生概要
   - 2012年（平成24年）の初夏から秋にかけて、日本において、犯人がネットの掲示板を介して他者のパソコンを遠隔操作し、これを踏み台としてウェブサイト、インターネット掲示板、メールを通じて襲撃予告や爆破予告などの犯罪予告を行ったサイバー犯罪。その犯人として4人が誤認逮捕された
2. 誤認逮捕が発生した原因
   - 書き込みに使用されたPCのIPアドレスと犯人として誤認逮捕された人のPCのIPアドレスが一致した
   - 複数のウィルス対策ソフトの検査では遠隔操作ウィルス（新種のトロイの木馬）の痕跡の発見は不可能であった
3. 誤認逮捕であることが判明した根拠
   - 逮捕後の押収したPCの解析で、犯人とされていたPCから遠隔操作ウィルスの1つである新種の トロイの木馬を検出した（このトロイの木馬は自分自身を削除する機能を備えているが、ある1人のPCはトロイの木馬が残っていた）
   - 真犯人を名乗る者からの犯行声明文

（出典） Wikipedia 「パソコン遠隔操作事件」

http://ja.wikipedia.org/wiki/%E3%83%91%E3%82%BD%E3%82%B3%E3%83%B3%E9%81%A0%E9%9A%94%E6%93%8D%E4%BD%9C%E4%BA%8B%E4%BB%B6

誤認逮捕事案の分析

- 利用者がPCを安全に利用（継続利用）する観点から本事案のIT系技術に関連する原因を以下に示す

（誘導）

- ウイルスが仕掛けられた不正プログラムをダウンロードするように誘導された

（検知）

- 新しいウィルス（トロイプログラム）のため、ウイルス対策ソフトウェアの最新の定義ファイルでもこのウイルスを検知できなかった
- ウイルスが自動で動作するため、ウイルスの挙動を利用者が認識することができなかった（三重県の事案を除く）

（痕跡）

- ウイルスの動作による掲示板への書き込みに関する痕跡が残ったままとなった
- ウイルス自体が削除されたため、ウイルス自体の痕跡が残らなかった

誤認逮捕事案の原因に対応するD-Case適用のポイント

＜適用にあたっての基本的な考え方＞

- PC利用にあたって、自身、および、対外的に影響を与えないための継続的な安全利用（注意義務の履行）のケースを明確化する

原因

（誘導）

- ウイルスが仕掛けられた不正プログラムをダウンロードするように誘導された

（検知）

- 新しいウィルス（トロイプログラム）のため、ウイルス対策ソフトウェアの最新の定義ファイルでもこのウイルスを検知できなかった
- ウイルスが自動で動作するため、ウイルスの挙動を利用者が認識することができなかった（三重県の事案を除く）

（痕跡）

- ウイルスの動作による掲示板への書き込みに関する痕跡が残ったままとなった
- ウイルス自体が削除されたため、ウイルス自体の痕跡が残らなかった

D-Case適用ポイント

PCの安全利用に関するD-Caseの適用

1. 安全利用を示すPC利用(動作）のモニタリング
   ・利用者、訪問したURLの履歴、キータイプ情報、ネットワーク上の通信記録などの可視化

   ⇒ PC利用に関する説明責任

2. PCの不審な挙動に対して外部との遮断（ネットワーク遮断）などの対応策の実施

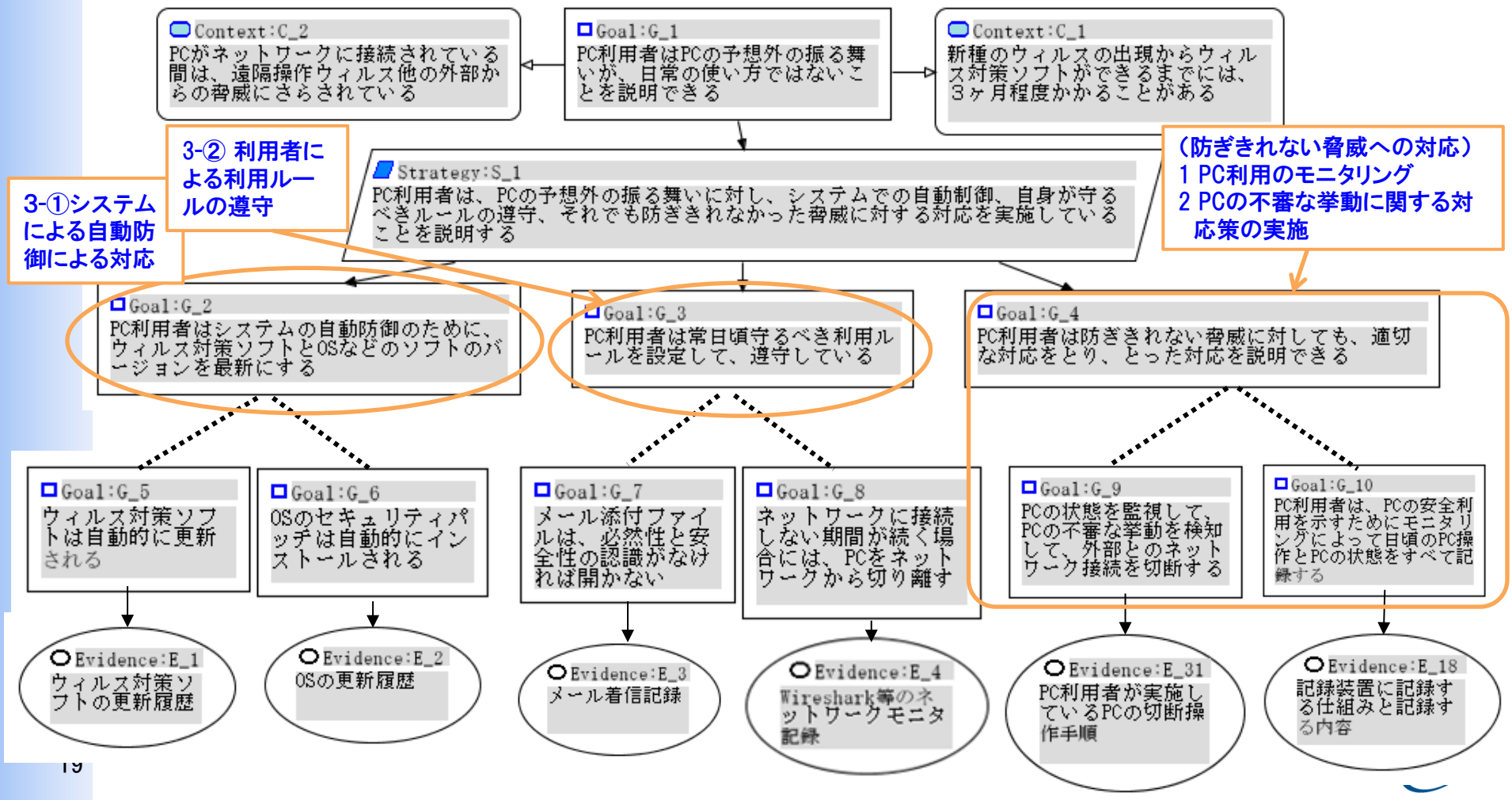
   ⇒ 脅威による影響の最小化

3. PCの安全利用のための対策の明確化
   ①システムによる自動防御
   1) ウイルス対策ソフトウェアの最新化と実行
      - ウイルス対策ソフトウェアの実行履歴
      - ウイルス定義ファイルの最新化の履歴、など（実行記録も含めた記録）
   2) ソフトウェアのセキュリティ対策のための最新化
      - セキュリティパッチの実施履歴

   ②利用者による利用ルールの遵守
   ・メール添付ファイルの安全確認、など

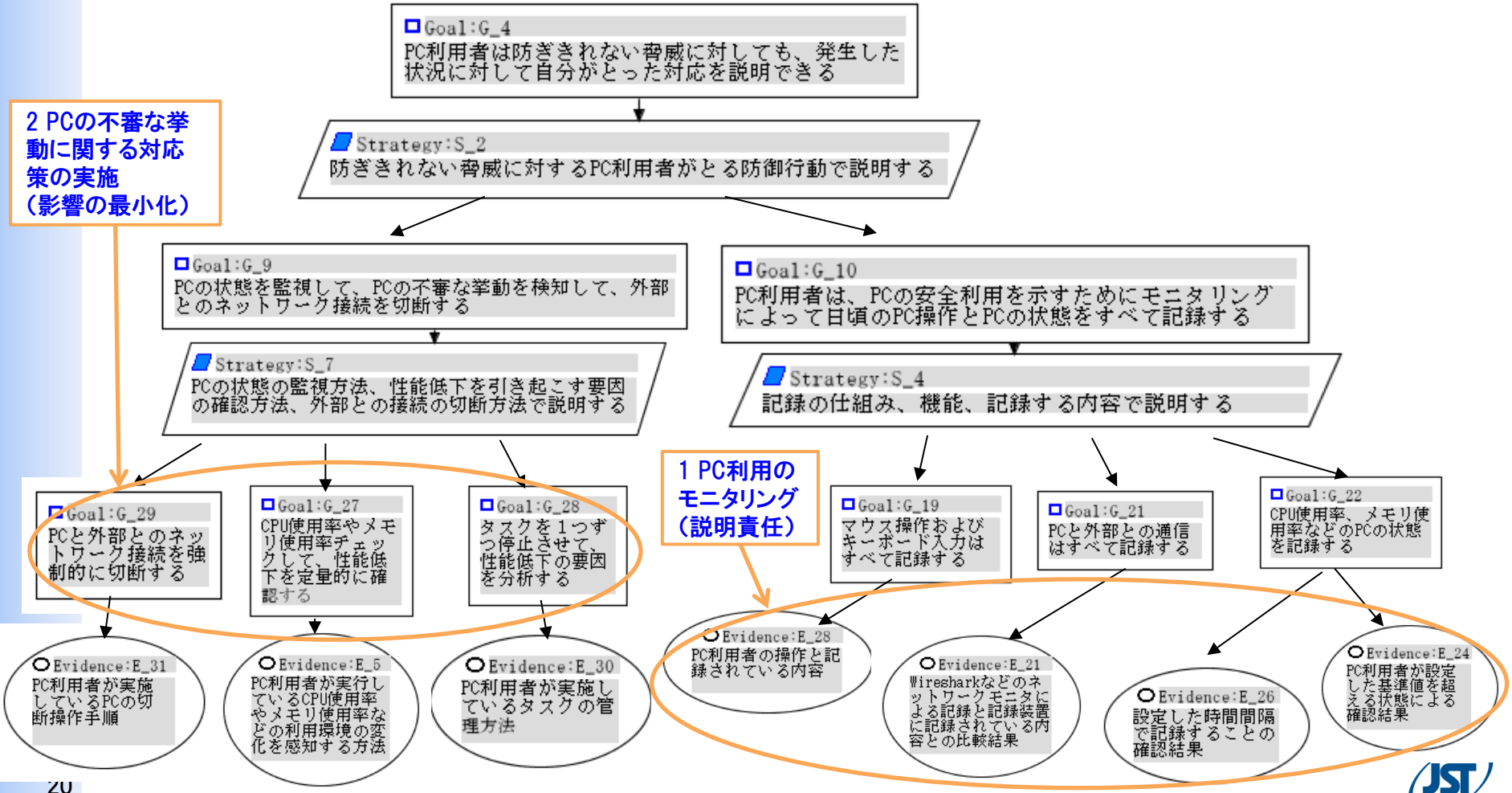
誤認逮捕事案へのD-Case適用時の有効性

- PCの予想外の振る舞いへの対応ケース展開
  - **防ぎきれない脅威への対応や日頃守るべき利用ルールの設定と遵守、システム機能としての自動防御の明確化と脅威の最小化**



誤認逮捕事案D-Case適用時の有効性

- 防ぎきれない脅威に対する説明責任と脅威の最小化
  - PC操作とPCの状態の記録によるエビデンスや、PCの不審な挙動に関する対応策の実施と影響の最小化



誤認逮捕事案へのD-Case適用のまとめ

D-Case適用
により

- 網羅性の可視化： システムによる自動防御だけでは対応することができない脅威を含めて、説明責任を果たすためのケースを可視化できる
  - （適用事例での例） PC利用者は自分の意図しないPCの振る舞いを証明できる
- 説明責任の明確化：PC利用のモニタリングによる説明責任の明確化
  - （適用事例での例）PC利用者は、PCの安全利用を示すためにモニタリングによって日頃のPC操作とPCの状態をすべて記録する
- 防ぎきれない脅威に対する影響の最小化行動：PCの不審な挙動に対する対応策の実施
  - （適用事例での例）PCの状態を監視して、PCの不審な挙動を検知して、外部とのネットワーク接続を切断する

その結果

- 自分の意図しない振る舞いに対する説明責任の実現
  （PC安全利用支援ツール（説明責任支援）の利用）
- システムによる自動防御では防ぎきれない脅威に対する影響の最小化の実現

D-Case事例　T証のシステム障害（2012年）の概要（1/3）

1.　株式売買システムの障害（2012年2月2日）

- **障害概要**
  - 情報配信ゲートウェイサーバーでハード障害が発生し、監視端末上に異常メッセージが表示され、異常メッセージへの対応を完了したが、株式売買システムの一部銘柄で相場情報が配信できない事象が発生。その後、ハード障害を契機とした予備系への切替え処理が正常に完了していないことが原因であると判明。当取引所の241銘柄及び他の券取引所を含む全74銘柄の売買を停止。システム障害の復旧作業を完了し、取引を開始。
- **再発防止措置**

1) 株式売買システムの障害発生に関する再発防止措置等
- ◆ 障害対応の体制面での改善及び強化
- ◆ 確認手順及び確認項目の明確化
- ◆ 速やかな復旧に向けた取組み
- ◆ 自動切替え発生時の動作確認

2) 本システムにおける切替え試験の実施
- ◆ 擬似障害再現による切替え機能及び対応フローの確認
- ◆ 全サーバーの切替え機能の確認

3) 再発防止策の他システムへの展開

D-Case事例　T証のシステム障害（2012年）の概要（2/3）

2.　デリバティブ売買システムの障害（2012年8月7日）

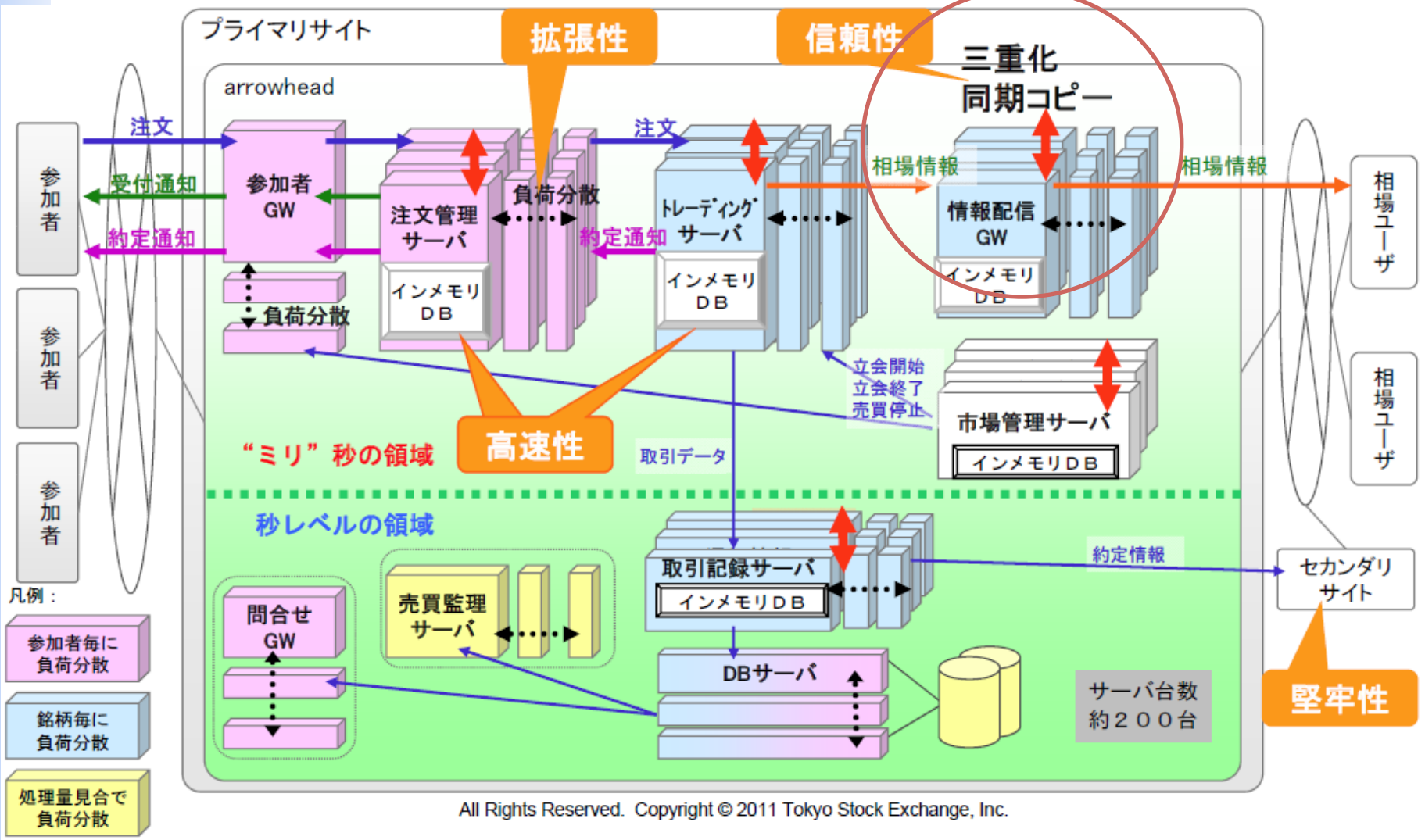
- **障害概要**
  - デリバティブ売買システムのネットワーク機器である業務L3スイッチの本番系（1号機）においてハードウェア障害が発生。直ちに障害対策本部を立ち上げ、障害の特定・復旧に向けた対応に着手したが、全派生商品の取引を停止。その後、システムの復旧作業を完了し注文受付・取引を再開
- **障害原因と対策**
  - 本番系（1号機）のハード障害に伴い、待機系（2号機）自体は本番系へ状態変更する自動切替処理を正常に動作させたが、1号機内部の部分的なハード障害検知の異常により、1号機、2号機の両方が、本番系の状態となった。その結果、これらスイッチに接続されている装置が送信先を特定することが不可能となり、通信ができなくなった。本不具合に係る製品内蔵プログラムの改修版のシステムへの取込みは、テスト環境での十分な検証を経た後に行う。なお、同様の事態備える対策を既に講じた。

D-Case事例　T証のシステム障害（2012年）の概要（3/3）

- 金融庁より業務改善命令を受け、再発防止策を発表
  - 未然防止の観点での施策（業務継続の観点から万一の場合を想定）
    - ◆取引停止につながる可能性の観点から機器の洗出し、切替えの仕組みや設計値の妥当性等確認（業務継続の視点）
    - ◆切替えが正常に機能しない場合の対策等について確認し、総点検を踏まえた改善施策の検討・対応の実施計画を策定（万一を想定）
    - ◆市販品の選定基準を策定
  - 障害発生時の業務影響を極小化するための施策
    - ◆障害発生時の初動体制の整備や障害テスト等を通じた担当者の教育及び訓練
    - ◆復旧作業を短縮し業務影響を極小化するため、障害発生時に対外影響のある、7システムを対象に障害時運用プロセスの再点検を実施

株式売買システムの概要

●1回目（2月2日）に障害が発生した情報配信ゲートウェイシステム（三重化による高信頼化）
（なお、2回目のシステム障害は、本システム図には含まない）



出典：ET2011講演資料より（「東証売買システム(arrowhead)のディペンダビリティ実現のための方式および機能」）

T証のシステム障害の分析

2度のシステム障害とも、サーバ、ルータの違いはあるものの、冗長構成での予備系への切り替え時の障害に起因するものであった。両障害とも、障害時の対応に課題があったと考えられる。

（1）冗長構成でのハードウェアの信頼性への過信（1回目の反省点）

- 障害遭遇を回避できるとの認識を前提とした考え方になっていた
- 人間系の役割を明確にしない（必要性を考慮しない）対応となっていた
- そのため、
  - 取引所主体でシステム状態を確認する運用がなされていなかった
  - 深夜・早朝時間帯の十分な監視体制が整備できていなかった
  - 経営陣への障害発生時の報告体制に不備があった

（2）サービスへの影響視点での対策の不備（2回目の反省点）

- システムの障害回避を中心に据えており、サービスへの影響回避の視点が欠けていた
- そのため、切替失敗時の復旧対応が迅速に行われなかった

T証のシステム障害の原因に対応するD-CASE適用のポイント

＜適用にあたっての基本的な考え方＞

- ハードウェア冗長構成での予備系切り替え時の障害においても継続的なサービスが実現できるようなケースを明確化する

原因

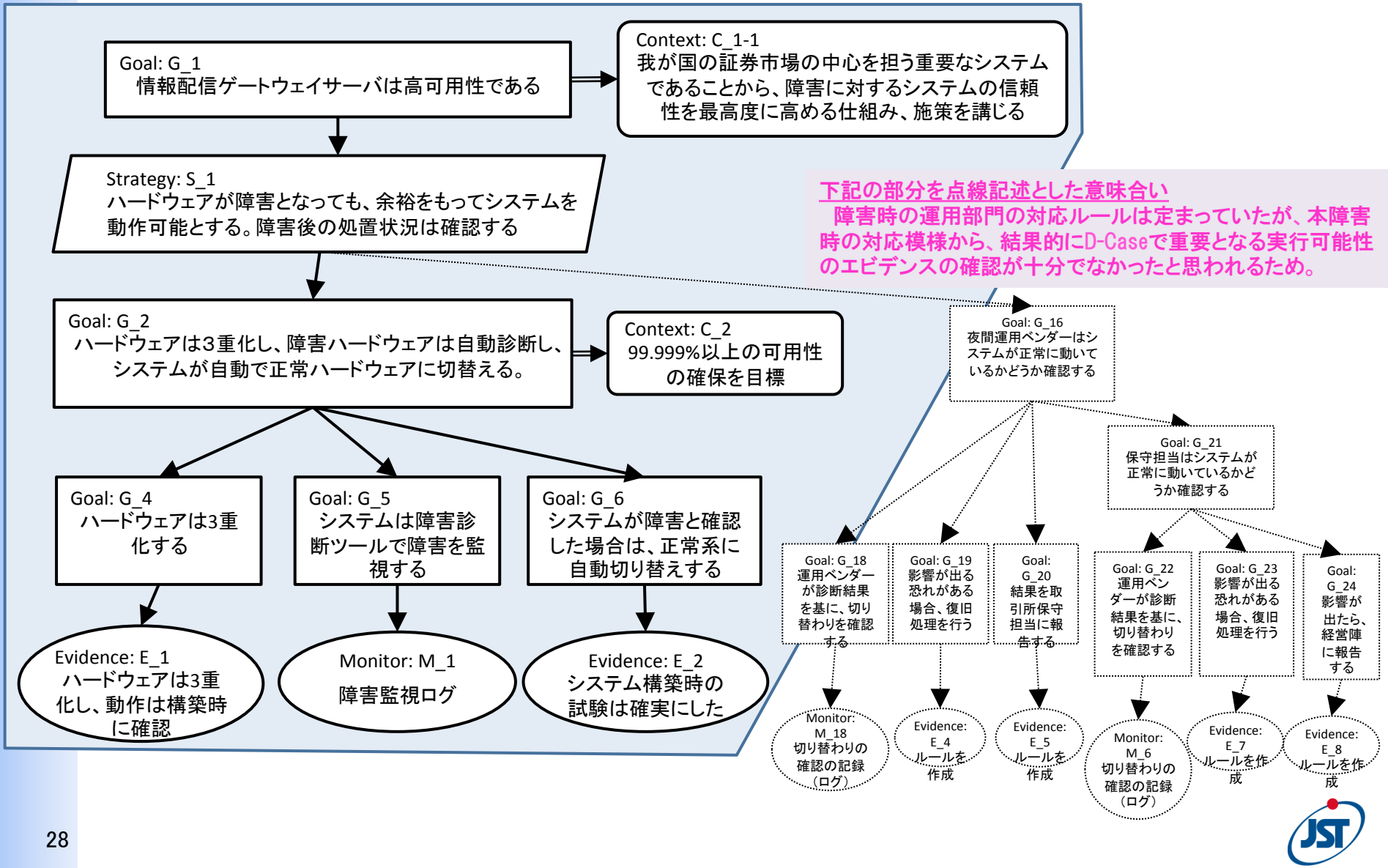
1. 冗長構成でのハードウェアの信頼性への過信（1回目の障害時）
   - 障害遭遇を回避できるとの認識を前提とした考え方になっていた
   - 人間系の役割を明確にしない（必要性を考慮しない）対応となっていた
   - そのため、
     - 取引所主体でシステム状態を確認する運用がなされていなかった
     - 深夜・早朝時間帯の十分な監視体制が整備できていなかった
     - 経営陣への障害発生時の報告体制に不備があった
2. 冗長構成時での予備系への切替が行われない場合の対策の不備
   - 1回目の障害対策では、システムの障害回避を中心に据えており、サービスへの影響回避の視点が欠けていた
   - そのため、切替失敗時の復旧対応が迅速に行われなかった

D-Case適用ポイント

1. 体制も含めた運用面の強化として、障害対応時の体制や運用の確認手順と確認項目、復旧手順等を明確化する（1回目の障害後の対応策）
   - 訓練の実施
   - 自動切り替え発生時の確認手順、など
2. 業務継続（未然防止策）や障害発生時の業務影響最小化の観点から運用を整備する（2回目の障害後の対応策）
   - 影響を最小化する障害時運用プロセスの整備
   - 製品選定基準の整備

D-Case適用時の有効性
①初回（2012年2月2日）の障害発生前の高可用性運用のD-Caseで記述

再発防止策の記載内容から、障害前の運用内容を抽出してD-Case形式で記述したもの

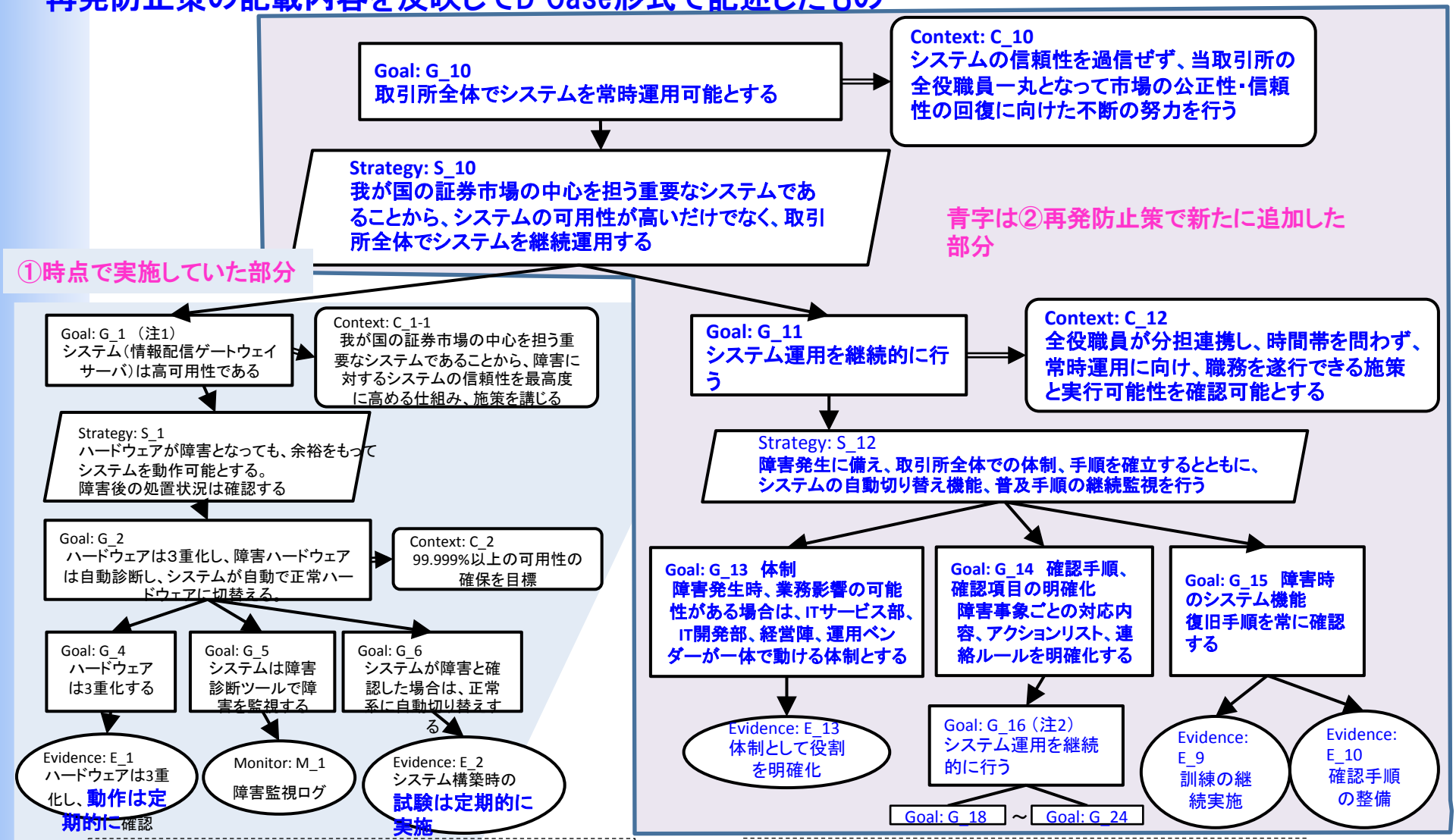


下記の部分を点線記述とした意味合い

障害時の運用部門の対応ルールは定まっていたが、本障害時の対応模様から、結果的にD-Caseで重要となる実行可能性のエビデンスの確認が十分でなかったと思われるため。

D-Case適用時の有効性
②初回(2012年2月2日)の障害発生後　防止策の常時運用のD-Caseで記述

再発防止策の記載内容を反映してD-Case形式で記述したもの



(注1)トップゴール(取引所全体でシステムを常時運用可能とする)を置くことにより、本ゴールをシステムの高可用性に拡張する

(注2)前頁の高可用性運用のD-CaseのGoal番号 G_16～G_24は、本ゴールと本ゴール以下のサブゴールとして記述される

4. D-Case適用時の有効性

③2012年8月7日の障害発生後の防止策　業務継続運用のD-Caseで記述

2012年8月7日の再発防止策の記載内容を反映してD-Case形式で記述したもの

青字は③で追加、修正した部分

Context: C_10
システムの信頼性を過信せず、当取引所の全役職員一丸となって市場の公正性・信頼性の回復に向けた不断の努力を行う

Goal: G_100
東証が提供する市場サービスは我が国証券サービスとして業務を継続（継続運用、影響の最小化、説明責任の全う）

Context: C_111
東証提供のデリバティブ市場、現物市場及びToSTNeT市場の3」サービスの注文データの流れを踏まえ施策を講ずる

Strategy: S_100
我が国の証券市場の中心を担う重要なシステムであることから、3サービスの取引停止につながる可能性の観点から機器の切替えが正常に機能しない場合を想定し、取引所全体で継続的に未然防止、影響の極小化を行う

③ ①②でも防ぎきれない場合でも業務継続するための対応

①システムによる自動防御による対応

②人が主体で動き、サービスの業務継続と継続改善

①時点で実施していた部分

Goal: G_1
システムは高可用性である

Context: C_1-1
我が国の証券市場の中心を担う重要なシステムであることから、障害に対するシステムの信頼性を最高度に高める仕組み、施策を講じる

Strategy: S_1
ハードウェアが障害となっても、余裕をもってシステムを動作可能とする。
障害後の処置状況は確認する

Goal: G_2
ハードウェアは3重化し、障害ハードウェアは自動診断し、システムが自動で正常ハードウェアに切替える。

Context: C_2
99.999%以上の可用性の確保を目標

Goal: G_4
ハードウェアは3重化する

Goal: G_5
システムは障害診断ツールで障害を監視する

Goal: G_6
システムが障害と確認した場合は、正常系に自動切り替えする

Evidence: E_1
ハードウェアは3重化し、動作は定期的に確認

Monitor: M_1
障害監視ログ

Evidence: E_2
システム構築時の試験は定期的に実施

②再発防止策で新たに追加した部分

Goal: G_11
システム運用を継続的に行う

Context: C_12
全役職員が分担連携し、時間帯を問わず、常時運用に向け、職務を遂行できる施策と実行可能性を確認可能とする

Strategy: S_12
障害発生に備え、取引所全体での体制、手順を確立するとともに、システムの自動切り替え機能、普及手順の継続監視、高信頼な製品調達を行う

Goal: G_13　体制
障害発生時、業務影響の可能性がある場合は、ITサービス部、IT開発部、経営陣、運用ベンダーが一体で動ける体制とする

Goal: G_14　確認手順、確認項目の明確化
障害事象ごとの対応内容、アクションリスト、連絡ルールを明確化する

Goal: G_15　障害時のシステム機能
復旧手順を常に確認する

Evidence: E_3
体制として役割を明確化

Goal: G_16
システム運用を継続的に行う

Goal: G_18 ～ Goal: G_24

Evidence: E_9
訓練の継続実施

Evidence: E_10
確認手順の整備

Goal: G_111
障害発生を防ぎきれなくても影響を極小化する

Strategy: S_111
注文等のデータの流れに沿って、取引停止の可能性のある機器を洗い出し、正常に機能しない場合の運用体制を整備する

Goal: G_112
製品選定基準を策定する

Evidence: E_11
選定基準の整備

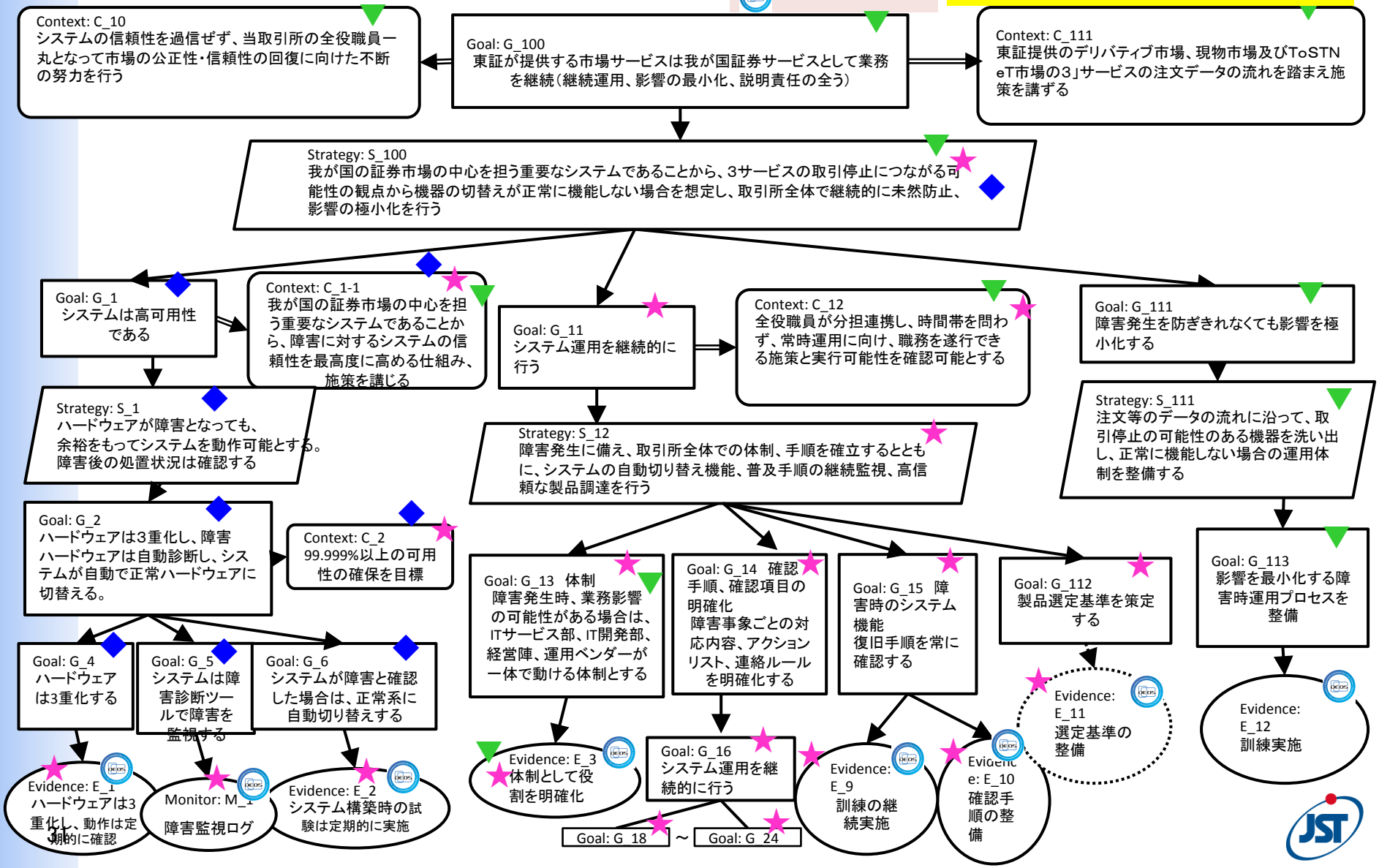
Goal: G_113
影響を最小化する障害時運用プロセスを整備

Evidence: E_12
訓練実施

D-Case適用時の有効性
④運用対応（D-Caseで記述）

主管部門
▼：経営層
◆：IT開発部門
★：ITサービス部門
：第3者機関など

システム関係は開発部、運用関係はサービス部門、社会に対する責任の全う経営層が掌握する。実行可能性の検証は、第3者機関などを想定した。



5. D-Case適用時のまとめ

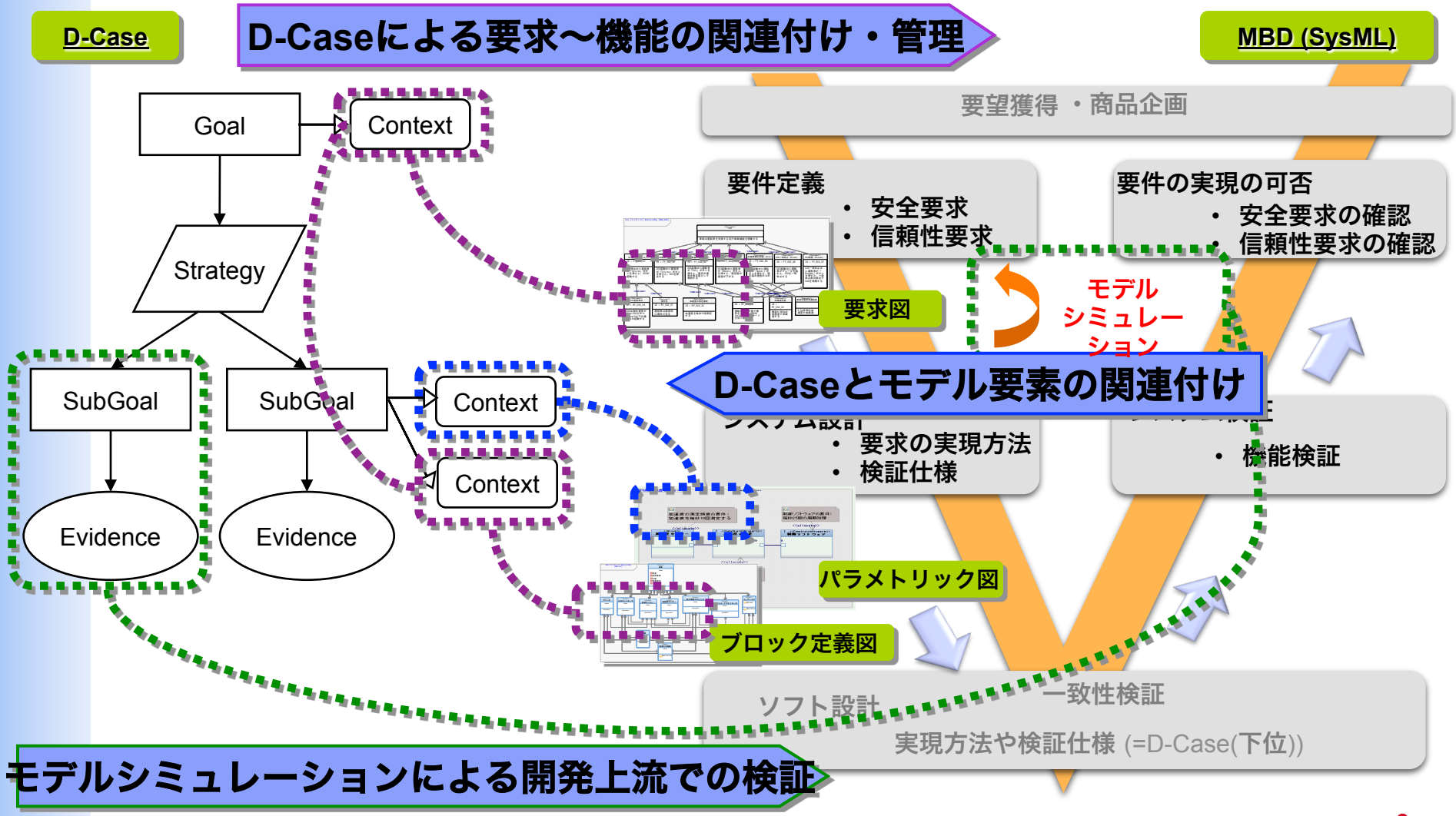
再発防止策から段階的に
D-Caseを適用することにより

- 業務継続・影響最小化の実現： ハードウェアの高信頼化だけでなく、業務継続性や障害時での影響最小化を目指すケースを可視化できる
  - （適用事例での例）「システム運用を継続的に行う」、「障害発生を防ぎきれなくても影響を極小化する」場合のケース（ゴール）を追加
- 役割分担の明確化： D-Caseで記述された各ゴールの責任部署を明確化できる
  - （適用事例での例） 経営層、IT開発部門、ITサービス部門、第3者機関などの役割
- 運用の実行可能性の検証： 体制や復旧手順などの手順確認や訓練結果などをエビデンスとして確認・検証できる
  - （適用事例での例）「体制としての役割の明確化」、「訓練の継続実施」等のエビデンス

その結果

- 業務継続のためのすべてのゴールや各組織の役割を一つのD-Caseドキュメントで表すことができる

D-CaseとSysML開発環境の連携 ― 概要



D-CaseとSysML開発環境の連携 ー 開発プロセスへのD-Case適用

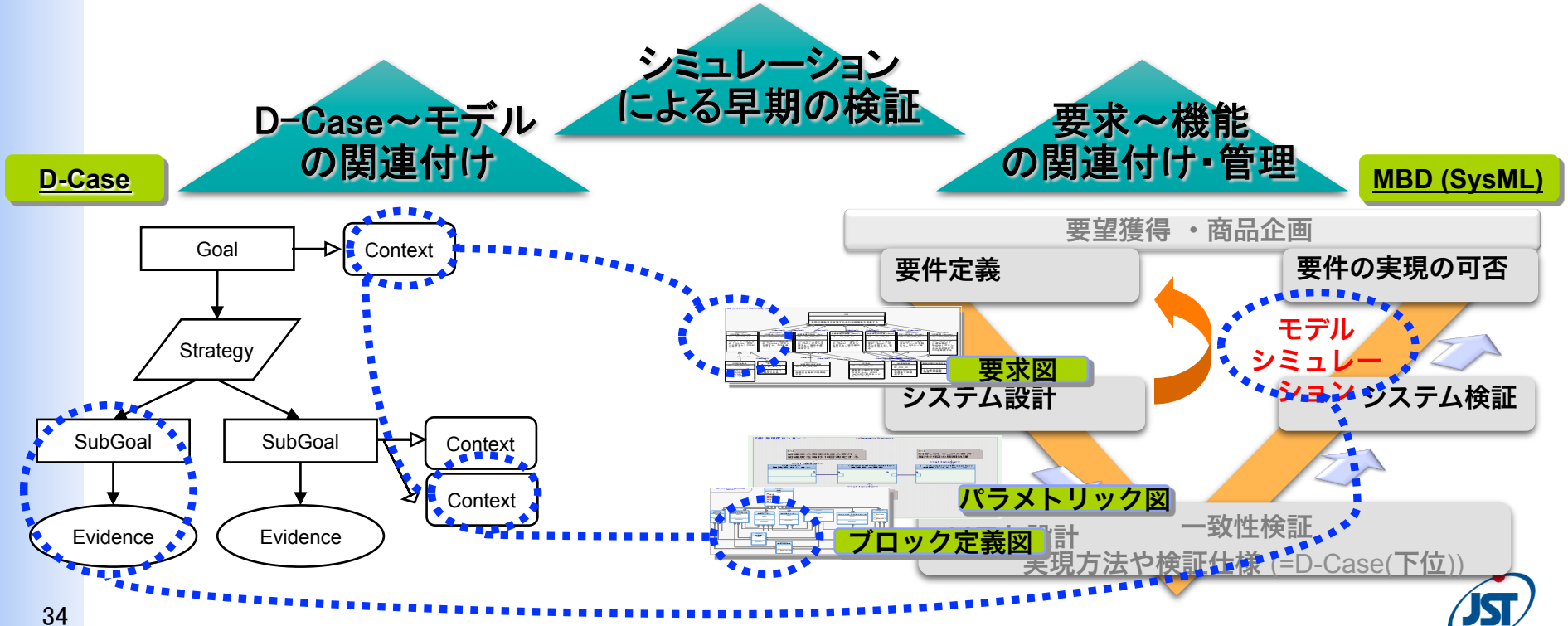
合意形成の達成

システムのディペンダビリティを利用者などの利害関係者に説明し納得してもらう

説明責任の達成

システムの開発・運用に当たって利用者などの利害関係者に説明すべきことを正しく説明する

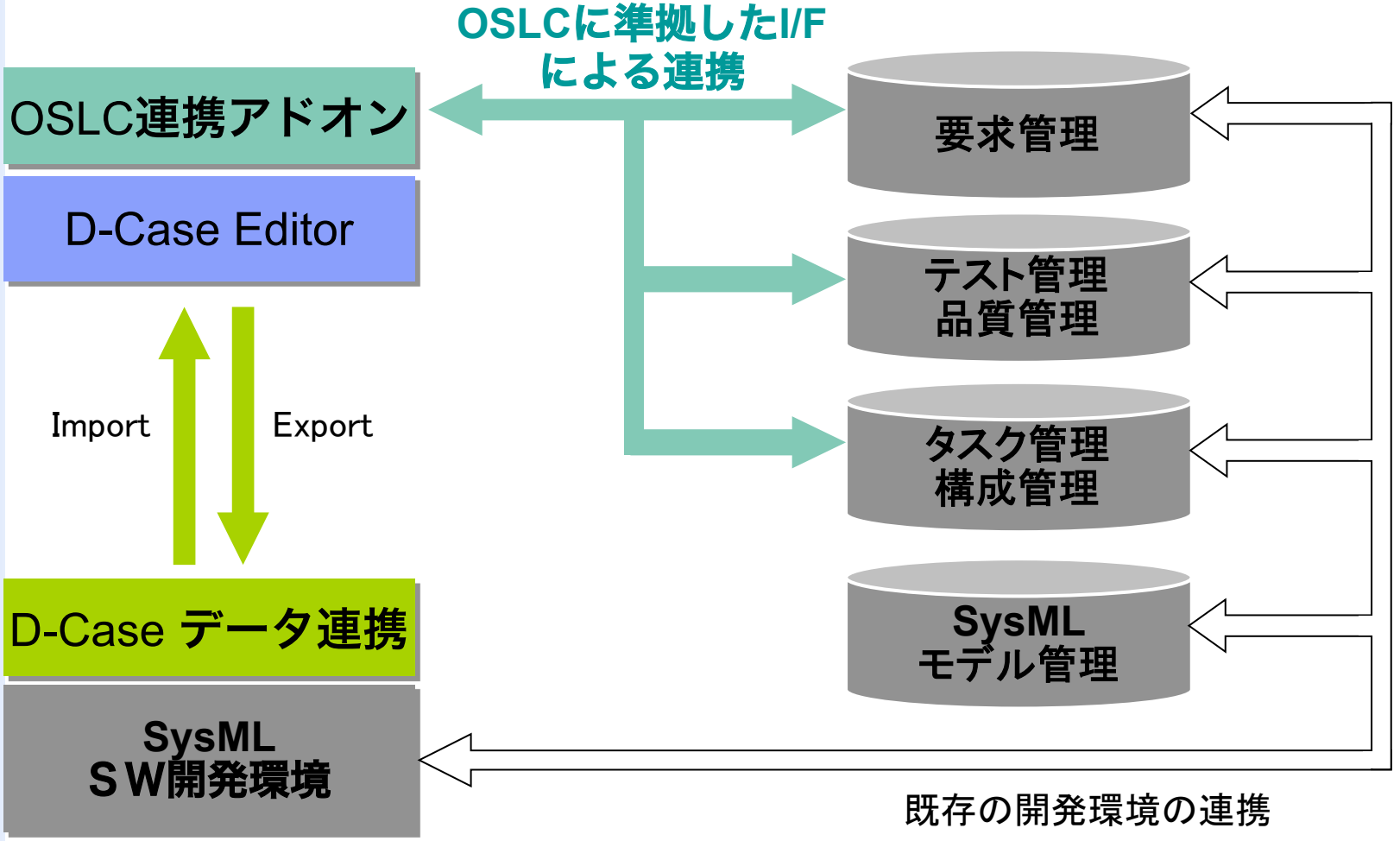
- 開発の上流で要求の妥当性を検証
- ゴールの達成に必要な要件・機能の関係を継続的に明確化



D-CaseとSysML開発環境の連携　－　開発環境システム構成

- D-Case Editor の OSLC連携アドオン
- SW開発環境の D-Case データ連携機能

OSLC (Open Services for Lifecycle Collaboration)
　異なるALMツール間でのデータ連携を可能とする
　仕様を策定



クルーズコントロールシステムの開発

自動車のクルーズコントロールシステム開発へD-Caseを適用

1. Dependability合意形成の手法・ツール
   D-Case
2. D-Case作成環境
   D-Case Editor
3. モデリング言語
   SysML
4. モデリング＆シミュレーション環境
   IBM Rational Rhapsody

D-CaseとSysML開発環境の連携　ー　まとめ

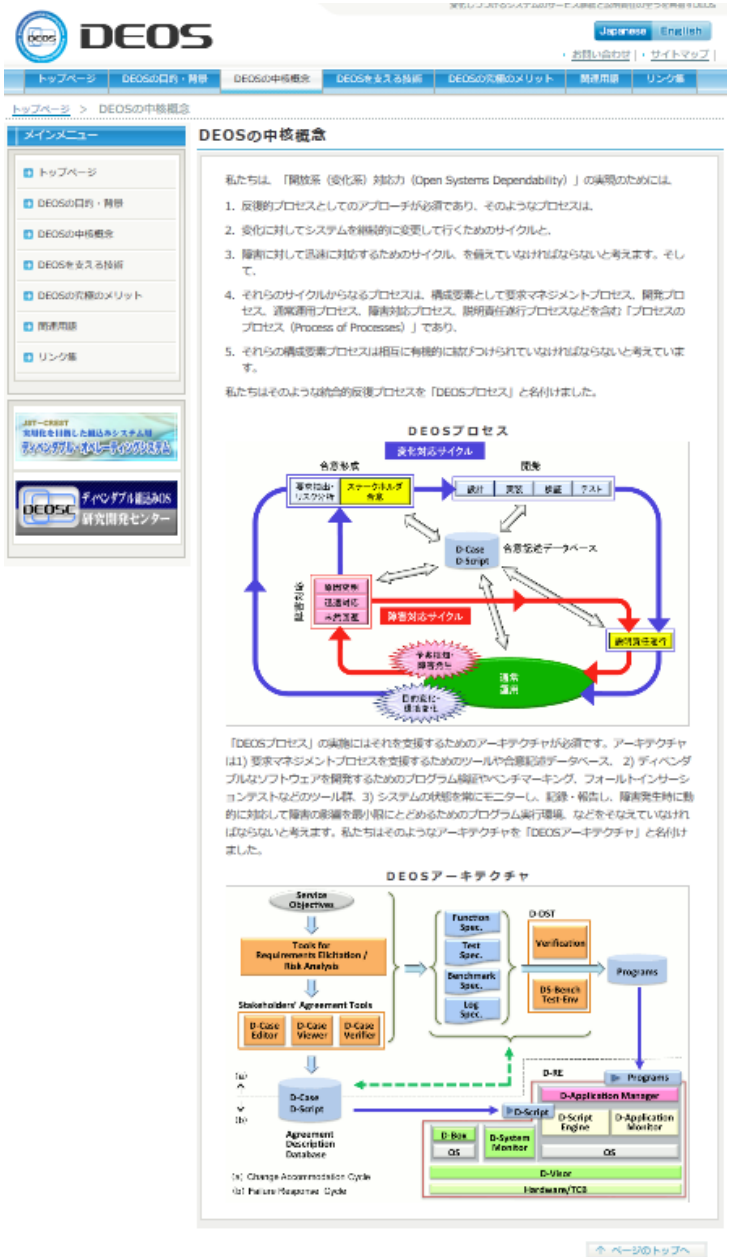
D-CaseとSysML開発環境の連携のメリット

- 開発の上流で要求の妥当性を検証できる
- ゴールの達成に必要な要件・機能の関係を明確化できる

連携機能の開発

- D-Case Editor の OSLC連携アドオンの開発
- SW開発環境の D-Case データ連携機能の開発

DEOS Homepage: http://www.dependable-os.net/



主なDEOS要素技術・ツール群

- ステークホルダ合意形成支援ツール
  -> D-Case Editor
- Webブラウザ版 D-Case Editor
  -> D-Case Weaver
- パワーポイント用 D-Case ステンシル
  -> D-Case Stencil
- D-Case整合性検査ツール
  -> D-Case/Agda
- D-Script （ D-Caseの記述を基にアプリケーションプログラムを動的に制御）
  -> 準備中
- D-ADD （ DEOS Process/D-Caseを支えるりポジトリー）
  -> 準備中
- ソフトウェア検証ツール
  -> モデル検査器
- D-Caseモデリング環境連携
  -> D-Case OSLC
- テスト支援ツール
  -> DS-Bench/Test-Env (DS-Bench/D-Cloud)
- シングルIPアドレスクラスタ
  -> Dependable Single IP Address Cluster (SIAC)
- 仮想マシンモニタとOS監視ツール
  -> D-Visor + D-System Monitor
- 改竄検知機能付き記録装置
  -> D-Box
- システムレコーダー
  -> System Recorder
- DEOSを実現するサービスを提供するための実行環境
  -> DEOS Runtime Environment (D-RE)

DEOS HP DEOSを支える技術:
http://www.dependable-os.net/osddeos/tech.html

標準化活動 ー IEC, ISO/IEC JTC1, OMG, & The Open Group

- IEC TC56 (Dependability)
  - NWIP提案: Open Systems Dependability 2012年9月提出
  - エキスパートとして改定作業に参加
    - IEC60300-1: Dependability management （最上位規格:Open Systemの概念）
    - IEC 62741: Dependability case
    - IEC 62628: Guidance on software aspect of Dependability
- ISO/IEC JTC1/SC7 (System and software engineering)
  - ISO/IEC15026: System and software assurance (co-editor)
- OMG (SysA: Systems Assurance Task Forceで活動)
  - “Machine Checkable Assurance Language”の提案
    - RFI (Requests for Information: 2012-09-04
    - 審議の後、Requests for Proposals, 投票を経て策定
  - “Dependability Assurance Framework for Safety-Sensitive Consumer Devices”の提案
    - IPA/SECコンシューマデバイスWG(委員長電通大新誠一教授)、トヨタ大畠氏らが中心となって提出
    - DEOSチームは標準化に協力
    - RFI (Requests for Information): 2011-12-02
    - White Paper: 2012-9-12
    - RFP(Request for Proposal): 2013.3発行、2013.11 Initial Submission
- The Open Group
  - RTES部会における標準化活動
  - Open Dependability Through Assuredness™(*) 標準V1.0発表 （2013年7月15日）
    - 公開ビデオ http://new.livestream.com/opengroup/allen-philly13/videos/24698802 （9分くらいから）

(*): Dependability Through Assuredness is a trademark of The Open Group

ET2013

■会場　：　パシフィコ横浜
■会期　：　11月20日（水）～11月22日（金）
■ブース展示　（小間番号）：　F-34

■スペシャルセッション（C-7）：　11月22日（金）10:00～14:00　アネックスホールF206
『オープンシステムディペンダビリティが世界える
～DEOS（変化しつづけるシステムのためのディペンダビリティ向上技術）、いよいよ実用化へ！』

10：00	開会挨拶　所　眞理雄（株式会社ソニーコンピュータサイエンス研究所）	
10：20	合意記述データベースと説明責任	横手　靖彦
10：45	D-Caseの実証評価の取組み	山本　修一郎
11：20	D-Caseとの連携を実現する運用スクリプト技法	倉光　君郎
11：45	D-Caseの移動ロボット適用事例紹介	加賀美　聡
12：10	Linuxのバグと惰弱性	河野　健二
12：45	DEOS実用化のためのオープンシステムディペンダビリティ国際標準化戦略	武山　誠・所　眞理雄
13：25	一般社団法人ディペンダビリティ技術推進協会の発足と今後の活動について	竹岡　尚三
14：00	終了予定	

ご挨拶

DEOSプロジェクト(*)は（独）科学技術振興機構の戦略的創造研究推進事業CRESTの研究領域として2006年に開始されました。これまで、組込みシステムのみならず、変更要求に対応しつつ継続して長期に運用しなければならないシステムや、他の管理者が運用するシステムと連携して稼働し続けなければならないシステムなどに対し、ディペンダビリティを向上するための概念、方法、システム、ツールなどを開発してきました。

このたび、このプロジェクトで研究開発された成果を広くご利用頂き、さらに発展させ、世の中のシステムのディペンダビリティ向上に貢献していくために、「一般社団法人 ディペンダビリティ技術推進協会（略称DEOS協会）」を発足することにいたしました。DEOS協会の活動を通じて、ディペンダビリティ技術の研究、開発、実証、評価、標準化などを推進し、皆様とともに安心、安全、快適な社会の構築に貢献したいと思います。皆様のご参加を心よりお待ちします。

2013年10月

一般社団法人 ディペンダビリティ技術推進協会　理事長
（独）科学技術振興機構DEOSプロジェクト研究総括
（株）ソニーコンピュータサイエンス研究所　エグゼクティブ・アドバイザー/ファウンダー

所　眞理雄

(*)DEOSプロジェクト：　正式名称は「実用化を目指した組込みシステム用ディペンダブル・オペレーティングシステム」です。

DEOS協会概要

法人概要

- 名称： 一般社団法人　ディペンダビリティ技術推進協会　（略称： DEOS協会）
  - 英語名称： The Association of Dependability Engineering for Open Systems (DEOS Association)
- 設立： 2013年10月（予定）
- 所在地： 京都市中京区烏丸通二条上ル蒔絵屋町280番地　インターワンプレイス京都8F　株式会社アックス　京都本社　内

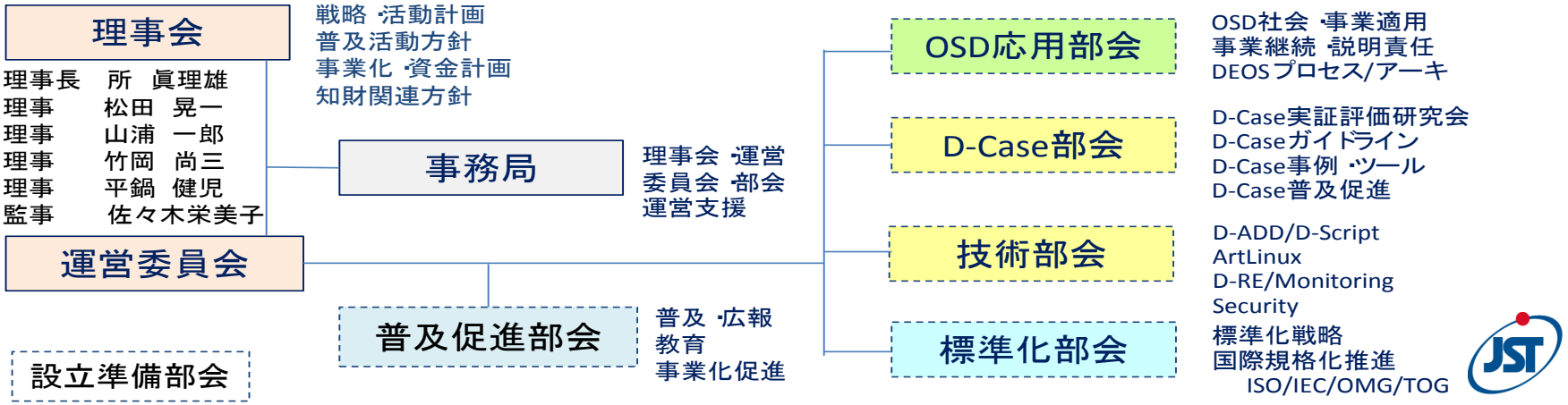
会員の種類・会費

- 正会員（入会金(*1)・年会費(*2)： 10万円）： 当協会の目的に賛同して入会する個人、法人またはその部署、団体またはその部署
- 賛助会員（入会金・年会費： 無償）： 当協会の事業を賛助するため入会する研究者個人、公共法人・公益法人等またはその部署、営利を目的としない団体またはその部署
- 学術会員（入会金・年会費： 無償）： 当協会に功労のあった者又は学識経験者で社員総会において推薦された者

発足までの問合せ先： （独）科学技術振興機構　ディペンダブル組込みOS研究開発センター

- E-mail: center@dependable-os.net
- 電話番号： 03-3526-6724
- URL: http://www.dependable-os.net/osddeos/index.html

(*1)　2013年度中の入会については入会金免除
(*2)　入会初年度に限り、年会費免除



発起人・連携予定団体

発起人

- 竹岡尚三（AXE）
- 平鍋健児（ChangeVision）
- 小阪暢之（ChangeVision）
- 波多野祥二（OTSL）
- 福富三雄（豆蔵）
- 黒田幸明（サイバー創研）
- 永山辰巳（Symphony）
- 浅井信宏（ DEOSプロジェクト研究推進委員、日本IBM）
- 大野毅（ DEOSプロジェクト研究推進委員、横河電機）
- 中川雅通（ DEOSプロジェクト研究推進委員、パナソニック）
- 森田直（ DEOSプロジェクト研究推進委員）
- 山浦一郎（ DEOSプロジェクト研究推進委員、富士ゼロックス）
- 加賀美聡（産総研）
- 木下佳樹（神大）
- 倉光君郎（横国大）
- 河野健二（慶大）
- 光来健一（九工大）
- 松野裕（電通大）
- 山田浩史（農工大）
- 山本修一郎（名大）
- 横手靖彦（慶大）
- 石川裕（東大）
- 佐藤三久（筑波大）
- 徳田英幸（慶大）
- 中島達夫（早大）
- 前田俊行（理研）
- 新誠一（電通大）
- 高田広章（名大）
- 平野晋（中大）
- 田丸喜一郎（IPA）
- 松原茂（JST）

連携予定の団体

- CSSC
- Terrace
- SVA
- JASA
- SMA
- AIST
- IPA
- JAXA
- JST

まとめ

- 新しいシステムディペダビリティの考え方が必要
- D-Caseを活用した体系化・ツール化されたプロセスの重要性が増大
- DEOSプロジェクトではD-Caseを広め活用するためのD-Caseツール群を提供
- D-Caseの活用方法や事例の紹介
- 既存の開発環境SysMLとの連携の試み
- DEOS関連のイベント、コンソーシアムのご紹介

JST/DEOS Center
http://www.dependable-os.net/index.html

JST/DEOS Project
http://www.crest-os.jst.go.jp/
http://www.jst.go.jp/kisoken/crest/research_area/ongoing/bunya04-4.html